ORACLE®

Statement of

Steven Perkins
Senior Vice President
Public Sector and Homeland Security
Oracle Corporation

Before the
Committee on Government Reform
United States House of Representatives

8 May 2003

Mr. Chairman, Ranking Member Waxman, and members of the Committee, thank you for the opportunity to appear before you today. My name is Steve Perkins and I am Senior Vice President of Public Sector and Homeland Security for Oracle Corporation.

It is only fitting that Oracle is represented today since the Ranking Member is from California – Oracle's home state -- and the Chairman is from Virginia -- the state where Oracle was founded and where our Government, Education, and Healthcare business are headquartered. In fact, many of my fellow Oracle team members who work in our Reston facility are proud to call the Chairman their Congressman. We are all very familiar with the Chairman's legislative accomplishments, such as the E-Gov Act, and the Critical Infrastructure Information Act; and we look forward to working with you in your new position of leadership in the Government Reform Committee.

Oracle was created twenty-six years ago to help the intelligence community manage its most sensitive information. Today, Oracle is the world's largest enterprise software company, providing information management software and expertise to firms that include 98 out of the Fortune 100, and to hundreds of departments and agencies in federal, state and local governments. Given our market penetration, we are an integral part of the nation's critical information infrastructure and, since September 11th, have worked with our customers, private and public, to better secure these vital networks. In fact Larry Ellison, our Chairman, led the first project, and remains actively engaged in innovations designed to improve the integrity and effectiveness of these systems. We at Oracle are proud to call the federal government a valued and strategic partner in these efforts

Mr. Chairman, I don't believe one can truly overstate the magnitude of the challenge facing Secretary Ridge, Steve Cooper and the entire Homeland Security team. Since the formal creation of the Department last March, the Department has been working very hard to stand itself up on a number of levels – personnel, administrative and technological – in order to have 22 federal entities and 190,000 federal employees work in a cohesive fashion. While not the largest of mergers on a commercial scale it is certainly one of the most complex I've seen in my career, and clearly one with the highest stakes for our nation.

Of course, Oracle monitors closely the investments made by Congress toward information technology, and how the Department, as well as other federal, state and local entities uses those investments to advance homeland security. Information is, after all, one of, if not the most powerful weapon that we have in the fight against terrorism. Just ask the brave men and women of our armed forces and intelligence agencies who served to liberate Iraq -- the more we know about the enemy, the more likely we are to be able to anticipate, prevent or effectively respond to his actions. A central concept of network centric warfare is making information available in near real time and pushing to the edges of the organization – a model to be emulated at DHS.

Strangely, when you watch the news shows, you get the sense that we don't have enough information. As someone who helps our customers manage information, I can say first hand that information is all over the place. The real problem is the capability needed to establish relationships between various information sources. Real knowledge is found in these relationships, not in the data itself. That was one of the tough lessons of September 11th. There were lots of "facts" out there about individual terrorists – the federal government was unable to bring these facts together so that intelligence agencies and law enforcement could see the whole picture.

We are very pleased that DHS CIO Steve Cooper is looking to establish an enterprise architecture for his Department, consistent with OMB policy. We are advocates of this approach. By establishing clear business processes and business flows as part of this enterprise architecture model, the DHS is in a better position to drive technology toward these objectives. The architecture can serve as the blueprint for information sharing vertically with state and local institutions, as well as horizontally among federal components both within and outside the Department.

That's one of the key challenges we are working on with the Transportation Security Administration. TSA is positioned to receive vast amounts of information, but its success will be based on how well this information is processed and presented in order for TSA to take action. For example, we are working with TSA to provide incident management and case tracking capabilities in order for TSA to better manage its information flows. Further, we are working with TSA on a public portal so that citizens can report suspicious activities with public transportation systems. Just as important, these systems offer business continuity and scalability.

We hope that the efforts now underway at TSA will serve as a blueprint for the kind of information management architecture needed in other homeland security agencies. One of the fundamental, positive lessons that can be drawn from the TSA example is the utility of an enterprise architecture approach – an approach that builds its systems infrastructure in stages, and enables the agency to do more with less through common databases, tools and resources.

Accomplishing this requires a commitment to standards, but not standards exclusive to the DHS, or standards set by Congress. For example, integration standards define how a system exposes its data to other systems. Industry-generated web services standards like WSDL, UDDI, and SOAP define how a system wraps up its data and publishes it to other systems. So a system can use these standards to say (in effect), "I know all about pilot licenses in the state of Florida. If you give me a social security number, I will check your credentials and then give you XML in the following format that includes that person's license information." This approach means that I don't care what a system does or how it was built. I only care that it can accept and answer my question.

Since federal, state, and local systems are all built independently, integration standards are necessary if they are going to be built or updated to effectively share information. We understand that Mr. Cooper is not going to insist on DHS exclusive standards, but work to integrate or reinforce existing standards, or leverage the DHS to push for industry developed and supported standards. This approach in the long run is cost effective for both the public and private sectors.

Perhaps the most important form of information standard is geared toward security. The most significant barrier to information sharing will most likely be driven by concerns raised by organizations – private and public -- about exposing their data to potentially insecure systems. There are well-established standards for securing data and auditing its use. These standards have matured around the world and are now accepted globally. In the United States, their use is managed by NIAP, the National Information Assurance Partnership – an effective collaboration between the National Security Agency and the National Institute of Standards and Technology. Together, they manage the standards and independent evaluations processes required to ensure that technology providers like Oracle are implementing secure products.

Oracle is one of a number of software companies that build security into its software development process, rather than bolting it on through a constant barrage of patches. A build-in, as opposed to a bolt-on approach to security produces better products. We even go the extra step and invest in having our software tested against internationally recognized information assurance standards, such as the Common Criteria.

Federal agencies — collectively the single largest buyer of commercial off-the-shelf software products — can change the marketplace for the better by making information assurance, through independent evaluations, a factor in their buying decisions. In January of 2000, a committee within the National Security Agency proposed that federal agencies with information systems involved in national security can only purchase commercial information assurance software that has been independently evaluated to be secure. This policy went into affect last July, and the Defense Department has developed regulations consistent with this policy, which Congress endorsed last year in its Defense authorization bill. Also, the President's cybersecurity strategy called for a study on the potential effectiveness of applying similar policies throughout the federal government.

I bring this issue to the Committee's attention because we at Oracle believe DHS should adopt this acquisition strategy. After all, if the tragic terrorist attacks of September 11 proved anything, it is that our most sensitive information systems in federal information sharing and coordination of strategies will likely take place among those law enforcement agencies within and outside of the Homeland Security Department. Information sharing and analysis also is likely to occur between our law enforcement and intelligence agencies. All of this activity requires that the Department have strong information assurance strategies, including those involving the purchase of information assurance systems in the commercial market.

Whether it's information security, enterprise architecture, or industry standards, the approaches taken by DHS necessitate the need for continued outreach with the private sector. When the White House first created the Office of Homeland Security, it instituted a very open, accessible, and in our estimation, effective outreach program to private sector innovators in the high tech community. Clearly, the challenges and demands of the newly created Department are far more complex and all consuming, particularly in the face of that complexity. It is essential that the Department, particularly Mr. Cooper, work hard to maintain that accessibility and visibility, and not just with vendors, but also with key customers in state and local governments, so they can better understand how they fit in the overall infrastructure. We believe the private sector can and must contribute quickly to solve the information and integration challenges.

As DHS moves forward with its proposed enterprise architecture, the need for continued openness is especially critical, particularly on the program side.

Finally, on a related topic, I wanted to touch on an issue that I know is important to the Chairman – a section in the Homeland Security Act called the Support Anti-terrorism by Fostering Effective Technologies Act – otherwise known as the SAFETY Act. This new law is designed to provide liability protections to private contractors that are producing qualified anti-terrorism technologies for federal, state or local governments. These protections are essential if we are to encourage innovative solutions to the numerous challenges that face both government and the private sector in securing our nation's homeland. The Chairman was instrumental in bringing this legislation to the attention of the Congress and in getting it included in the Homeland Security Act.

In order to receive this liability protection, a contractor's product has to meet several important criteria. The SAFETY Act will require regulations to further clarify product eligibility, but as of yet, draft regulations have not been issued. I am sure a number of our partners in the technology community would agree with me that the sooner we can get these regulations available to the public for comment and then finalized, the sooner we can encourage forward-thinking ideas to protect our critical infrastructures and most important, to best implement a homeland security strategy.

In conclusion, Mr. Chairman, I believe the Department is making sound, measurable progress on information integration. No doubt, individual entities that are part of our overall homeland security infrastructure are focusing on getting their own systems and capabilities up and running, and will press Congress to fund individual systems. What we risk in that kind of a situation is a thousand well-funded little systems, but no improved national capacity to deal with the threat of terrorism. This would amount to a failure of planning and protection. The DHS is working with the private sector, and state and local governments to make sure that doesn't happen. Congress, as policy leaders, can best assist the DHS by defining appropriate policies to guide federal, state and local organizations down a common path of better information sharing. The information technology industry can devise the systems to make sure these policies can work, despite government differences, to accomplish our national goals.

Thank you again for the opportunity to testify today. I look forward to answering any questions you may have.